

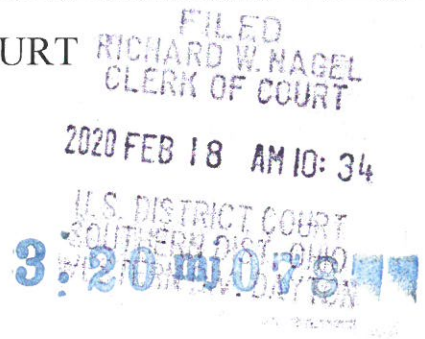
UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Four Cellular Telephones

Case No.



APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 USC s. 846	conspiracy to distribute and possess with intent to distribute controlled substances
21 USC s. 841(a)(1)	possession with intent to distribute controlled substances

The application is based on these facts:

Attached Affidavit of Austin M. Roseberry

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 2/18/20

City and state: Dayton, Ohio

Applicant's signature
Austin M. Roseberry, SA of the DEA
Printed name and title
Judge's signature
Michael J. Newman, US Magistrate Judge
Printed name and title

AFFIDAVIT

Austin M. Roseberry, a Special Agent (S/A) of the Drug Enforcement Administration (DEA), United States Department of Justice ("hereinafter referred to as the Affiant"), being duly sworn, deposes as follows:

INTRODUCTION

1. Affiant is an "Investigative or Law Enforcement Officer" of the United States Drug Enforcement Administration within the meaning of Title 21, United States Code, Section 878. That is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 21, United States Code, Section 878.

2. Affiant is a law enforcement officer and has been employed by the DEA since July 2012, and is currently assigned to the Dayton Resident Office. Affiant has conducted and participated in complex drug trafficking conspiracy and money laundering investigations which have resulted in arrests; execution of search warrants that resulted in the seizure of narcotics, narcotics proceeds and other evidence of narcotics trafficking activities; and supervised the activities of cooperating sources (CS) that have provided information and assistance resulting in narcotics purchases. Through training and experience, affiant is familiar with the manner in which persons involved in the illicit distribution of controlled substances often operate. These people usually attempt to conceal their identities, as well as the locations at which they reside, and where they store controlled substances and the illegal proceeds derived there from. Through training and experience, affiant is familiar with the practices of narcotics distributors, whereby they attempt to conceal the true nature, source and location of proceeds of illegal activity, commonly referred to as money laundering. Affiant has participated in several Title-III wire tap investigations and is familiar with how local drug traffickers and high level traffickers conduct transactions.

3. This Affidavit is submitted in support of an Application for Search Warrants authorizing the search of the following electronic devices, more particularly described in Attachment A, incorporated herein by reference, for the items described in Attachment B, incorporated herein by reference: Purple Apple iPhone marked as N-25; Silver Apple iPhone marked as N-26; Red Apple iPhone marked as N-27; and Black Apple iPhone marked as N-28 (collectively, the "Subject Devices").

4. As outlined below, there is probable cause to believe that violations of Title 21, United States Code, Sections 841(a)(1) and 846 (possession with intent to distribute and to distribute controlled substance as well as the conspiracy to do the same) are being committed, and that evidence, fruits, and instrumentalities of these violations as set forth more fully in Attachment B, is presently located in the SUBJECT DEVICES.

5. Affiant is participating in an investigation conducted by agents of the DEA and other agencies, into the methamphetamine and fentanyl distribution activities of individuals in the Dayton, Ohio area, and elsewhere. Fentanyl and methamphetamine are schedule II controlled substances. I am familiar with the facts and circumstances described herein and make this affidavit based upon personal knowledge derived from my participation in this investigation, conclusions I have reached based on my training and experience, and upon information I believe to be reliable from the following sources:

- A. Physical surveillance conducted by federal and local law enforcement agents, the details of which have been reported to me either directly or indirectly;
- B. Information developed from cooperating sources and/or defendant witnesses;
- C. Public records;

This affidavit does not contain all facts known to Affiant, only those necessary to establish probable cause in support of the request of a search warrant for cellular telephones described above.

FACTS SUPPORTING PROBABLE CAUSE

6. On February 12, 2020, Detective Chris J. Savage observed a gray Jeep Compass with Pennsylvania registration in the area of Delaware Avenue and Richmond Avenue in the City of Dayton, Ohio. Detective Mark D. Orick was in a marked Dayton Police Department cruiser and conducted a traffic stop on a gray 2019 Jeep Compass, with Pennsylvania registration KXT2704, as it was pulling in the driveway of 626 Kenilworth Avenue, Dayton Ohio 45405. Detective Orick initiated the traffic stop due to a turn signal violation.

7. Upon initiating the traffic stop the driver of the Jeep Compass, Robert Miller Jr. exited the vehicle started to approach Detective Orick's cruiser. Detective Orick ordered the driver, Robert Miller III onto the ground. Mr. Miller failed to follow Detective Orick's directions and had to be placed on the ground by Detective Orick. As Detective Orick was securing Robert Miller III, the front passenger, described as a slender black male wearing all black clothing opened the door and exited the vehicle. The front passenger then fled through the front yard of 625 Kenilworth Avenue and into the backyard of 617 Kenilworth Avenue. Detective Erick M. Hamby, who was arriving on scene, initially ran after the front seat passenger toward the rear of the residence. Detective Hamby called out the direction of the male fleeing over the radio and returned to the vehicle to assist Detective Orick. Detective Orick then removed the rear passenger Nicholas Bell from the rear of the Jeep Compass. Both the driver Robert Miller III and Nicholas M. Bell were secured in Dayton Police cruisers.

8. Detective Hamby then followed the path that the front seat passenger took after fleeing the vehicle. Upon going around the garage in the rear of 617 Kenilworth Avenue, Detective Hamby located a green wrapped package that was like and similar to how

narcotics are packaged in a “Kilo” size unit. It was free of any debris and appeared to have just been dropped there. The crystal substance in the green package was field tested with methamphetamine test kit and turned blue indicating the presence of methamphetamine.

9. Investigators conducted a probable cause search of the Jeep Compass and located two cellular phones. Investigators located a red iPhone (Exhibit N-27) between the front passenger seat and the center console. Investigators located a black iPhone (Exhibit N-28) plugged into a charger in the back seat where BELL was sitting. Investigators located two additional iPhones (Exhibit N-25 and N-26) that fell from MILLER III’s pocket while Detective Orick was attempting to handcuff MILLER III. Law enforcement maintained custody of the Subject Devices in Dayton, Ohio.

10. Based on affiant’s training and experience, affiant uses the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety

of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

e. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

11. Based on training and experience, your Affiant knows that drug traffickers frequently use wireless/cellular phones to carry out their activities. They use cellular phones to communicate with customers, their associates, and their suppliers. It is often common for drug traffickers to have multiple phones because certain phones may be used only for certain purposes. For instance, a trafficker may use one phone just to speak to his supplier, while using a different phone to speak only to his customers. This is a counter-surveillance technique intended to make it harder for law enforcement to identify the user of the phones and his associates. Traffickers commonly use prepaid cellular phones to hide their identity as the user because they generate no billing information, often require little to no identifying information to activate, can sometimes be activated using an alias, and can be easily disposed of should the trafficker believe that law enforcement has identified the phone number.

12. Your Affiant also knows that traffickers commonly text message each other or their customers, such as meeting locations, prices, and other information needed to carry out the sale of drugs (sometimes in code). They commonly store phone numbers for their associates and customers in the electronic phone book/contacts list, often under alias or code names. Your Affiant knows that traffickers, using digital cameras located on their cellular phone, will sometimes use the cellular phone to take photographs or videos of themselves, their location, their product, their firearms or their associates, which can be electronically stored on the cellular phone. Information can also be downloaded from the internet onto the cellular phone, such as email, social network information (like "Facebook"), travel information like maps or directions, or photographs. Call data, such as missed calls, received calls, or dialed calls are often electronically stored in the cellular phone. The information electronically stored on a phone can also be evidence of who possessed or used a cellular phone at a given time, can contain direct evidence of drug trafficking acts, and can help identify drug trafficking locations or associates through GPS data. Affiant is aware that there are tools to extract electronic data from a cellular phone so that law enforcement can review it for items of evidentiary value.

13. In this modern era, individuals also use smart telephones and smart devices to logon to online banking platforms. I know that drug traffickers often use banking services to transmit money to their domestic and international suppliers.

14. Based on my knowledge, training, and experience, your Affiant knows that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

15. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the subject devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the subject devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge

about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.


e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

16. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Subject Devices onsistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.


17. Manner of execution. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

18. Based on the above, your Affiant submits that there is probable cause to believe that SUBJECT DEVICES will contain phone numbers, text messages, and other electronically stored information related to the possession with intent to distribute controlled substances, and the conspiracy to do the same, as well as information related to drug trafficking associates and other evidence of drug trafficking activity. Therefore, your Affiant respectfully requests that a search warrant be issued so that investigators can retrieve the electronic data from the SUBJECT DEVICES.


Austin M Roseberry, Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me

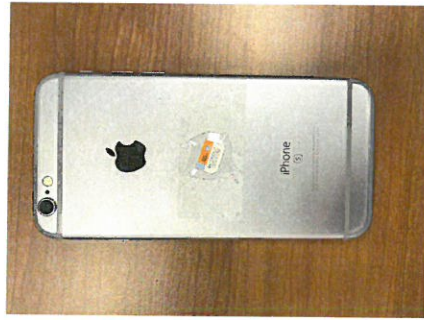

Honorable Michael J. Newman
United States Magistrate Judge

ATTACHMENT "A"

1. Purple Apple iPhone marked as N-25



2. Silver Apple iPhone marked as N-26



3. Red Apple iPhone marked as N-27



4. Black Apple iPhone marked as N-28



ATTACHMENT B

ITEMS TO BE SEIZED

Evidence of a crime—namely, violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute and to distribute controlled substances); and 21 U.S.C. § 846 (conspiracy to possess with intent to distribute and to distribute controlled substances). Items to be seized include, but are not limited to, the following documents, digital media, electronic data and records:

1. Call histories, voicemails, contacts or other call logs and information relating to or concerning drug trafficking activity or the sale of illegal drugs including, but not limited to: drug quantities; drug prices; drop locations for money or narcotics; the location of stash houses or bank accounts; the identity or contact information for coconspirators; the purchase, possession or acquisition of assets such as cars, homes, or jewelry; directions to meeting locations.
2. Text messages, SMS, or other written communications or information concerning or relating to the trafficking or distribution of narcotics, including, but not limited to: drug quantities; drug prices; drop locations for money or narcotics; the location of stash houses or bank accounts; the identity or contact information for coconspirators; the purchase, possession or acquisition of assets such as cars, homes, or jewelry; directions to meeting locations.
3. Photographs, videos or other electronic media relating to or depicting the trafficking or distribution of illegal drugs, including, but not limited to: firearms, bulk cash, illegal drugs, associates or other coconspirators, homes or potential stash houses.
4. Financial information, including, but not limited to, bank account information, wire transfer information, or other information in any form relating to the movement of currency or cash.
5. Evidence of user attribution, including any matter establishing indicia of ownership or use of the cellular telephones, including, but not limited to, photographs, videos, text messages, contacts, call history, logs, phonebooks, saved usernames and passwords, documents, and browsing history.
6. GPS history or applications that have map functions or provide driving directions, which may provide information relating to the location of stash houses or the locations of conspirators.
7. Records evidencing the use of any Internet Protocol address to communicate with any website, including records of Internet Protocol addresses used and records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.